UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/917,368	07/27/2001	Jeffrey Scott Bardsley	RSW920010137US1	1486

7590 02/05/2008

Duke Yee
Yee & Asscoiates P C
4100 Aipha Road
Suite 1100
Dallas, TX 75244

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
02/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

9

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/917,368
Filing Date: July 27, 2001
Appellant(s): BARDSLEY ET AL.

Theodore Fay III
Reg. #48,504
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/13/2007 appealing from the Office action mailed 6/12/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,973,040	RICCIULLI	12/2005
6,553,005	SKIRMONT	4/2003

Hunt et al., "Network Dispatcher: a connection router for scalable Internet services", 10/2/1998, Internet Security Systems

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 5-10, 15, and 18-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Ricciulli (U.S. Patent 6,973,040).

Regarding Claim 5,

> Ricciulli discloses a computer-implemented method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:
>
> Obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system (Column 3, lines 16-33);
>
> Obtaining network information, from network equipment connected to the device, regarding the attack (Column 4, line 45 to Column 5, line 2);

Determining a logical entry point (IP addresses, as well as TCP/UDP ports are logical representations used in combination to identify the entry point) of the attack using a correlation engine to correlate the intrusion information and the network information (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2); and

Identifying a physical entry point (the physical entry point is where the router or node actually connects to the network, on it's network interface) associated with the logical entry point (Column 3, lines 34-43).

Regarding Claim 6,

Ricciulli discloses that the intrusion information includes an address (Column 3, lines 16-33).

Regarding Claim 7,

Ricciulli discloses that the address is a source address (Column 4, line 65 to Column 5, line 2).

Regarding Claim 8,

Ricciulli discloses that the address is a destination address (Column 3, lines 16-33).

Regarding Claim 9,

Ricciulli discloses that the network information includes a logical port identifier of a logical port associated with the address (Column 4, line 65 to Column 5, line 2).

Regarding Claim 10,

Ricciulli discloses that the step of determining a logical entry point includes the step of finding, in the network information, the logical port identifier of the logical port associated with the address (Column 3, lines 29-43; and Column 4, line 45 to Column 5, line 2).

Regarding Claim 15,

Ricciulli discloses that the network equipment includes a firewall with routing function (Column 3, lines 16-28; and Column 4, lines 45-64).

Regarding Claim 18,

Ricciulli discloses that the intrusion detection equipment includes network based intrusion detection equipment (Column 5, lines 3-26).

Regarding Claim 19,

Ricciulli discloses that the intrusion detection equipment includes host based intrusion detection equipment (Column 3, lines 29-33).

Regarding Claim 20,

Ricciulli discloses that the intrusion detection system includes application based intrusion detection equipment (Column 5, lines 27-37).

Claims 11, 17, and 21-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ricciulli in view of Skirmont (U.S. Patent 6,553,005).

Regarding Claim 11,

Ricciulli discloses that the step of identifying a physical entry point includes the step of identifying an interface associated with the logical port

(Column 3, lines 34-43); but may not explicitly disclose identifying a physical port associated with the logical port.

Skirmont, however, discloses identifying a physical port associated with the logical port and/or identifying a physical port associated with an interface (Column 4, line 66 to Column 5, line 67). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network device and mapping methods of Skirmont into the intrusion detection system of Ricciulli because such mapping is well known in the art and/or to maintain packet flows from a common source to a common destination to be routed along strict physical paths, thereby allowing for efficient detection and filtering of attacks, and/or to provide the system with efficient load balancing, thus protecting against packets being received out of order and consequently being lost/discarded.

Regarding Claim 17,

Ricciulli does not disclose that the network equipment includes a load balancer.

Skirmont, however, discloses that the network equipment includes a load balancer (Column 5, lines 52-67). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network device and mapping methods of Skirmont into the intrusion detection system of Ricciulli because such mapping is well known in the art and/or to maintain packet flows from a common source to a common destination to be routed along strict physical paths, thereby allowing for efficient detection and filtering of attacks, and/or to provide the system with efficient load balancing, thus protecting against packets being received out of order and consequently being lost/discarded.

Regarding Claim 21,

Ricciulli discloses a method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the device being one of a plurality of devices connected by a network, the method comprising the computer-implemented steps of:

Detecting an attack on the device (Column 3, lines 16-33);

Notifying a correlation engine of the attack on the device (Column 3, lines 16-33);

Obtaining intrusion information regarding the attack (Column 3, lines 16-33);

Obtaining network information regarding the attack (Column 4, line 45 to Column 5, line 2);

Using the correlation engine, correlating the intrusion information and the network information to produce correlation information (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2);

Using the correlation information, finding on the network a logical port of connection used by the attack (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2); and

Mapping the logical port on the network to an interface on the network using the correlation engine (Column 3, lines 34-43); but may not explicitly disclose identifying a physical.port associated with the logical port.

Skirmont, however, discloses identifying a physical port associated with the logical port and/or identifying a physical port associated with an interface (Column 4, line 66 to Column 5, line 67). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network device and mapping methods of Skirmont into the intrusion detection system of Ricciulli because such mapping is well known in the art and/or to maintain packet flows from a common source to a common destination to be routed along strict physical paths, thereby allowing for efficient detection and filtering of attacks, and/or to provide the system with efficient load balancing, thus protecting against packets being received out of order and consequently being lost/discarded.

Regarding Claim 22,

Ricciulli as modified by Skirmont discloses the method of claim 21, in addition, Ricciulli discloses alerting a network manager to the location of the logical port and of the physical port (Column 3, lines 16-50).

Regarding Claim 23,

Ricciulli as modified by Skirmont discloses the method of claim 21, in addition, Ricciulli discloses that the step of mapping is performed using the correlation engine (Column 3, lines 34-43).

Regarding Claim 24,

Ricciulli as modified by Skirmont discloses the method of claim 21, in addition, Ricciulli discloses that the intrusion information includes an address (Column 3, lines 16-33); and the network information includes a logical port identifier of a logical port associated with the address (Column 4, line 65 to Column 5, line 2).

Regarding Claim 25,

Ricciulli discloses an apparatus for detecting a point of an attack on a network, the apparatus comprising:

Network equipment for connecting a protected device to a network (Column 3, lines 16-28);

An intrusion detection system comprising intrusion detection equipment (Column 3, lines 16-33);

A correlation engine (Column 3, lines 16-43; each of the system's routers contains this correlation engine, used to determine the entry point of an attack based upon stored and received information) adapted to:

Receive a notification of an attack on the protected device (Column 3, lines 16-33);

Receive intrusion information regarding the attack (Column 3, lines 16-33);

Receive network information regarding the attack, wherein the network information pertains to the network (Column 4, line 45 to Column 5, line 2);

Correlate the intrusion information and the network information to produce correlation information (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2);

Use the correlation information to find on the network a logical port of connection used by the attack (Column 3, lines 16-43; and Column 4, line 45 to Column 5, line 2); and

Map the logical port on the network to an interface on the network using the correlation engine (Column 3, lines 34-43); but may not explicitly disclose identifying a physical port associated with the logical port.

Skirmont, however, discloses identifying a physical port associated with the logical port and/or identifying a physical port associated with an interface (Column 4, line 66 to Column 5, line 67). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network device and mapping methods of Skirmont into the intrusion detection system of Ricciulli because such mapping is well known in the art and/or to maintain packet flows from a common source to a common destination to be routed along strict physical paths, thereby allowing for efficient detection and filtering of attacks, and/or to provide the system with efficient load balancing, thus protecting against packets being received out of order and consequently being lost/discarded.

Regarding Claim 26,

Ricciulli as modified by Skirmont discloses the apparatus of claim 25, in addition, Ricciulli discloses means for alerting a network manager to the location of the logical port and the physical port (Column 3, lines 16-50).

Regarding Claim 27,

Ricciulli as modified by Skirmont discloses the apparatus of claim 25, in addition, Ricciulli discloses that the intrusion information includes an address (Column 3, lines 16-33); and the network information includes a logical port identifier of a logical port associated with the address (Column 4, line 65 to Column 5, line 2).

Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ricciulli in view of ND (Hunt et al., "Network Dispatcher: a connection router for scalable Internet services", 10/2/1998, Internet Security Systems, obtained from http://www.unizh.ch/home/mazzo/reports/www7conf/fullpapers/1899/com1899.htm).

Ricciulli does not disclose that the network equipment includes a network dispatcher.

ND, however, discloses that the network equipment includes a network dispatcher (Pages 1-2, Introduction, Paragraphs 1-4). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network dispatcher of ND into the intrusion detection system of Ricciulli in order to allow the system to protect a broader range of network equipment, thus increasing the types of routers that can be used and protected by the system, and to reach those customers that use network dispatchers.

(10) Response to Argument

A. Response to arguments regarding claims 5-11, 15, and 18-20, rejected under 35 U.S.C. 102 as being anticipated by Ricciulli. Appellant included claims 21-27 in the header of this argument, however, claims 21-27 were rejected under 35 U.S.C. 103 in the last office action.

Regarding claim 5, Appellant provides 2 main arguments (page 10). One argument being that Ricciulli does not teach determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information; and the other argument being that Ricciulli does not teach identifying a physical entry point associated with the logical entry point.

How the determining step works is further shown by claim 10, in that "the step of determining a logical entry point includes the step of finding, in the network information, the logical port identifier of the logical port associated with the address." This logical port identifier is included in the network information (claim 9, from which claim 10 depends). Therefore, determining the logical entry point comprises finding the logical port identifier within the network information. Ricciulli (Figure 3, and column 4, line 45 to column 5, line 2, for example), explicitly shows finding, in the list(s) of network information, the logical port associated with the attack. This is performed by matching the intrusion information to the list(s) of network information to determine if a correlation is found. Ricciulli describes that "There are many possible network characteristics that can be matched in 3150. For example, IP source addresses 330, destination IP addresses 335, source TCP ports 340, source UDP ports 345, destination TCP ports 350, destination UDP ports 355, TCP flags 360, and/or ICMP flags 365" (column 4, line 65 to column 5, line 2). As seen here, any or all of this information may be correlated between the intrusion information and the list(s) of network information, this information including TCP and UDP ports, which Appellant admits are logical entry points (page 17, for example). Since more limiting claim 10 describes the determining step as finding the logical port identifier of a logical port within the network information, and Ricciulli teaches finding the logical port identifier of a logical port within the list(s) of network information, Ricciulli must teach the broader determining step of claim 5.

After this determining is completed within Ricciulli, the most upstream device that had seen the attack traffic (and implements the system) is identified as the physical entry point. Since this physical entry point had seen the attack traffic and had network information regarding such traffic in its list(s)/cache, that physical device/entry point must be associated with the logical entry point that was determined as just described.

As described below, the physical entry point may be either the current node or the downstream neighbor, as shown in column 3, lines 39-47.

Once this physical entry point is found, filtering may be put into place on such physical device/entry point. This is shown in column 3, lines 57-58 and column 4, lines 50-61. Column 3, lines 57-58 shows that, in one embodiment, "Filtering rules can be dynamically installed on an identified entry point", and the column 4 section shows more details about such filtering. Since such filtering rules are installed on an identified entry point, the entry point must have been identified, and it must be a physical entry point since the filtering rules are installed on the entry point. This physical entry point on which the filtering rules may be installed is associated with the logical entry point, as described above.

Appellant argues that Ricciulli does not even discuss logical entry points, except in the context of UDP ports and TCP ports (page 11). What must be determined, here, is what a logical entry point is. Appellant describes a possible entry point being the physical router that is the source of the attack (page 12). Since this is a physical device, this is a physical entry point of an attack. Within Ricciulli, this physical device can be identified by its interface information. This interface is associated with an IP address when Ricciulli is working at the IP level (column 3, line 10, for example). An IP address is a logical address used to identify the device. Since the device can be considered a physical entry point and the IP address can be a logical address associated with the physical device, the IP address must be a logical entry point. Additionally, the logical entry point can be any logical point of entrance through which packets corresponding to an attack travel, such as IP address or IP address/TCP port combination, for example.

Appellant also argues that, whether or not IP addresses and TCP/UDP ports are logical entry points is irrelevant, and what is relevant is determining a logical entry point of an attack (page 12). In order for something to be an entry point of an attack, it must first be an entry point. Therefore, it is entirely relevant that IP addresses and TCP/UDP ports may (singularly or in combination) be entry points. Additionally, Ricciulli is entirely concerned with determining and identifying entry points of an attack, as seen throughout the description.

Appellant also argues that no comparison is made to determine a logical entry point of the attack (page 13). As described above, Ricciulli explicitly teaches comparing intrusion information to network information in order to determine a logical entry point of the attack. This comparison may be performed on many possible network characteristics, including IP source and destination addresses, UDP and TCP source and destination ports, and TCP or ICMP flags.

Appellant describes that, in Ricciulli, a network/host address in an attack packet can be compared to a list of addresses in a router. If a match exists, then a message is sent to the next router upstream, whereupon the procedure repeats. When the final router does not find the address in its local cache, it sends a message to the return address in order to identify the final router as the entry point of the attack. While this is some of the functionality of Ricciulli, this is performed when the forwarded message stream reaches an upstream router that does not implement the forwarding and correlating mechanism. When a forwarded message is received by an upstream router that implements the mechanism and does not find the network/host address in its local cache, it will send a response indicating that its downstream neighbor is the entry point of the attack. Since the message that was sent to this current router by its downstream neighbor can be an IP packet (column 3, line 10, for example), containing both source (downstream neighbor) and destination (current router) IP addresses (IP packet headers can be seen in section 3.1 of RFC791, for example), the logical addresses of both the current router and its downstream neighbor have been determined via use of a correlation engine (the message is sent when the downstream neighbor had matched the intrusion information with network information, and thus has seen the attack traffic, prompting the forwarding to the current router). Since the current router is sending a response including the interface information of the downstream neighbor (which is associated with the IP address of the neighbor), the system has thus identified a physical entry point (interface information) associated with the logical entry point (IP address in this example). This could also be applied to the current router sending back a report packet indicating its interface information, which is associated to its IP address. The use of IP addresses in this form may be in addition to the correlation and identification as described with respect to claim 10 above.

Appellant argues that the Examiner misunderstands what a logical entry point is and states that a logical entry point is a virtual “port” maintained by a computer’s operating system (page 17). Appellant goes on to invite the Board to review an article provided by Symantec, describing a logical entry point as being:

"**Port**: Logical entry point of a network to your operating system. The operating system has 65,535 logical entry points that can be used by applications to communicate with the outside. Some are "opened" when requested during an outgoing connection, for example, whereas others can remain open permanently to accept connections coming from the outside."

As one will note, this is a definition for a port, and not a logical entry point. However, Appellant still concludes "Thus, an Internet address is not a logical entry point, as asserted by the Examiner." Many portions of Appellant's arguments rely on the incorrect belief that a logical entry point must be a port. This faulty logic of inferring that an address cannot be a logical entry point because the definition for a port states that a port is a logical entry point is analogous to stating that an apple cannot be a fruit because a pear is defined as being a fruit.

One will additionally note that this definition for port clearly and explicitly states that a port is a "logical entry point." Therefore, if one were to take this as a binding definition of a port, it would be impossible for a port to be a physical entry point, only a logical entry point. If this were the case, Appellant's claim 11 would not be possible, since claim 11 states that "the step of identifying a physical entry point includes the step of identifying a physical port". At best, this definition is relevant only within the context of the Symantec article from which it was taken.

Appellant also argues, regarding claim 5, that Ricciulli "does not correlate the logical entry point of attack to a physical point, as claimed" (page 18). Claim 5 does not, however, claim correlating a logical entry point of an attack to a physical entry point.

Claim 5 does recite "identifying a physical entry point associated with the logical entry point." This does not inherently involve correlation, however, only identification of the physical entry point "associated with" the logical entry point. As described above, Ricciulli clearly and unambiguously teaches identifying a physical entry point associated with the logical entry point.

As claim 5 was used as the representative claim for those claims rejected under 35 U.S.C. 102 as being anticipated by Ricciulli, claims 6-11, 15, and 18-20 have the same arguments and an equivalent response.

B. Response to arguments regarding claims 11, 17, and 21-27, rejected under 35 U.S.C. 103 as being unpatentable over Ricciulli in view of Skirmont.

Appellant argues that Skirmont is related to routing packets outwardly from a router, as opposed to obtaining intrusion information into the router (page 22). While Skirmont is primarily related to routing packets to egress ports, column 8, lines 7-10 shows that "physical ports in routers may both transmit and receive packets, and inventors herein have described primarily one-way operation. This is a convenience only, and not a limitation of the invention." Therefore, the physical ports that are associated with the logical ports may also receive packets, as well as transmit them. Additionally noted is that an entry point of attack need not necessarily be an ingress port into a router, as described above, such an entry point can be an IP address, a physical device, source or destination ports, etc. The mere fact that Skirmont refers to "egress ports" throughout most of the description is insignificant, since the combination teaches all limitations of the pertinent claims.

Appellant argues that Skirmont notes a destination address and consults a forwarding table (page 23). Indeed, the destination address can be one of the factors in determining which port to send the data to, but other characteristics may be used. For example, column 5, lines 52-67 of Skirmont clearly shows sending packets having the same source and destination address pair to exactly the same physical port. Other characteristics may be used than just addresses, as seen in column 3, lines 52-64, for example.

Appellant argues that the examiner appears, possibly, to cite Skirmont solely for the proposition that mapping logical ports to physical ports is known (page 23). While such a mapping is certainly well known, the Examiner did not simply cite Skirmont for showing that mapping logical ports to physical ports is known. Rather, the combination was viewed, as a whole, and it was determined that incorporating the network device and mapping methods of Skirmont into the intrusion detection system of Ricciulli provides many advantages, as will be described below.

Appellant argues that Skirmont teaches away from the claims (page 24). As basis for this argument, Appellant describes that Skirmont is directed towards finding egress points, while claim 11 is directed towards finding a physical entry point of attack. As described above, Skirmont teaches using the physical ports for both transmission and reception of data. Additionally, when considering the obviousness rejection of claim

11, one must look at the combination, instead of one reference individually, the combination in this case being directed towards finding entry points of attacks.

Appellant argues that the examiner failed to state a prima facie obviousness rejection against claim 11 because the examiner failed to state a proper reason to achieve the legal conclusion of obviousness under the standards of KSR (page 24). Since a finding of a teaching, suggestion, or motivation to combine the references is a valid rationale for determining obviousness, the Examiner providing a motivation to combine the references is a proper establishment of obviousness. In this case, there are multiple motivations for combining the network device and mapping system of Skirmont into the intrusion detection system of Ricciulli, including the fact that mapping of logical ports to physical ports is well known (Skirmont, column 5, lines 40-41), and/or to maintain packet flows from a common source to a common destination to be routed along strict physical paths (Skirmont, column 2, lines 20-25), thereby allowing for efficient detection and filtering of attacks, and/or to provide the system with efficient load balancing, thus protect ting against packets being received out of order and consequently being lost/discarded (Skirmont, column 1, lines 41-50).

This incorporation of the network device and mapping methods of Skirmont into the intrusion detection system of Ricciulli provides many benefits. By forcing packets of the same flow to be routed along strict physical paths, attack packets with the same characteristics will be routed through the same path. This is greatly beneficial since it leaves the other paths open for legitimate traffic while attack traffic is saturating a certain path. Skirmont, column 3, lines 52-64 shows determining ports based on common characteristics of packets, such as addresses or labels. Additionally, by providing such strict paths, the system can determine which nodes and ports are affected by an attack. By using such routing and mapping within Ricciulli, legitimate traffic will be sent to a different port and through a different path than attack traffic, and such legitimate traffic will be received in order, thereby further enhancing a legitimate user's experience. Furthermore, the forwarded (and reporting) messages of Ricciulli may be specified to belong to distinct routes and ports, thereby ensuring their delivery, even when the network is under a denial of service attack.

Appellant argues that Ricciulli and Skirmont address different problems (page 25). Both Ricciulli and Skirmont are concerned with determining which routes packets with certain characteristics take. As just described, by incorporating the network device and mapping methods of Skirmont into the intrusion detection system of Ricciulli, distinct advantages are brought forth.

Appellant argues that the Examiner used impermissible hindsight when combining the references (page 27). In response to Appellant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the Appellant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Appellant also argues, with respect to claim 17, that the proposed combination does not teach or suggest all of the features of claim 17 (page 28). As described above, Ricciulli clearly and unambiguously teaches all of the limitations of claim 5. Since claim 17 depends from claim 5, and Skirmont teaches a load balancer in the form of a router, the combination of Ricciulli-Skirmont teaches all of the limitations of claim 17.

As claim 11 was used as the representative claim for claims 11, 17, and 21-27, claims 17 and 21-27 have the same arguments (except as noted with regard to claim 17) and an equivalent response.

C. Response to arguments regarding claim 16, rejected under 35 U.S.C. 103 as being unpatentable over Ricciulli in view of ND (hereafter referred to as Hunt).

Appellant argues that Ricciulli as modified by Hunt does not teach all of the limitations of claim 16 (page 30). As described above, Ricciulli teaches all of the limitations of claim 5. Since claim 16 depends from claim 5, and Hunt teaches a network dispatcher, the combination of Ricciulli-Hunt teaches all of the limitations of claim 16.

Appellant argues that the examiner failed to state a prima facie obviousness rejection against claim 16 because the examiner failed to state a proper reason to achieve the legal conclusion of obviousness under the standards of KSR (page 31). Since a finding of a teaching, suggestion, or motivation to combine the references is a valid rationale for determining obviousness, the Examiner providing a motivation to combine the references is a proper establishment of obviousness. In this case, the motivation is to allow the system to protect a broader range of network equipment, thus increasing the types of routers that can be used and protected by the system, and to reach those customers that use network dispatchers. Companies use network dispatchers in order to keep the processing load evenly spread or balanced on a group of servers. By using a network dispatcher as one of the routers within Ricciulli, the ability to detect and protect against attacks expands to allow protection of network dispatchers as well as other forms of routers. This is clearly beneficial so that the combination can now be used on networks upon which companies have placed network dispatchers. As described, for example, in the client affinity portion (section 6) of Hunt, a network dispatcher can additionally provide the same advantages that were described with regard to Skirmont (all packets from a certain source taking a certain route, etc.).

Appellant argues that no rational reason to achieve the legal conclusion of obviousness in view of Ricciulli and Hunt exists because they address different problems (page 32). Ricciulli discusses a system that transfers data between routers. Hunt discusses a particular kind of router and how it transfers data. Since both Ricciulli and Hunt are concerned with routers and the forwarding of data from/to routers, Ricciulli and Hunt are analogous art.

Appellant argues that the Examiner used impermissible hindsight when combining the references (page 34). In response to Appellant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the Appellant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Jeff Popham
Patent Examiner, GAU 2137

Conferees:

Gilberto Barron
SPE 2132

GILBERTO BARRON Jr
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

/Benjamin E. Lanier/
Benjamin E. Lanier
Primary Examiner, GAU 2132